REMARKS

Applicants thank the Examiner for the thorough consideration given the present application. Claims 1-27 are currently being prosecuted. The Examiner is respectfully requested to reconsider his rejections in view of the Remarks as set forth below.

Amendments to Claims

Applicants have amended claims 4 and 5 to change their dependency so that proper antecedent basis is now provided. Claim 6 has been amended to remove an obvious informality. Claim 10 has also been amended to remove a possible informality by the use of "such as" language. No new issues are believed to be involved with these changes.

Rejection under 35 U.S.C. § 103

Claims 1-9, 12, 13, 18, 23, 26 and 27 were rejected in the final rejection under 35 U.S.C. § 103 as being obvious over Rowney et al. (U.S. Patent No. 5,987,140) in view of Oishi (U.S. Patent 6,298,153). This rejection is respectfully traversed.

Applicants have now amended claim 1 to clarify the point that the legal entity B validates the transistory insignia thorough legal entity C. Also, it has now been clarified that the legal entity C invalidates the insignia. Applicant submit that this amendment helps to clarify the operation of the device and the flow of control between the three entities.

Applicants again disagree with the Examiner's understanding of the references and submit that claim 1 is not obvious this combination of references. The Examiner has referred to

column 11, lines 30-37 to show the verification of the approval of the legal entity B. Applicants disagree that this reference teaches this arrangement. As indicated in column 11, lines 14-17, the merchant computer system transmits a service certificate to authenticate the identity of the merchant computer system. Column 11, lines 30-37 indicate that the customer computer system transmits a client certificate to the merchant computer system. This authenticates the identity of the customer computer system. Each of these certificates is generated by the computer which it attempts to authenticate. This is different from the present invention where entity A obtains an insignia from entity C so as to verify its approval to entity B. Accordingly, Applicants submit that the flow of the certification is completely different than that of the present invention. Accordingly, Applicants submit that the certification described in Rowney et al. is different from that of the unique transistory insignia as is presently claimed. Furthermore, the flow of the authentication is different from that of the reference.

The Examiner admits that Rowney et al. does not teach the use of the transistory insignia for a single transaction and that it is valid only for a time to complete the transaction. The Examiner relies on Oishi to teach these features. The Examiner refers to column 18, lines 33-43, to teach this concept. This section of column 18 does indicate that an anonymous public key certificate can be used one time. However, the present unique transistory insignia is not an anonymous public key certificate. At best, Oishi only teaches the concept that it is possible for a certificate to be used one time and discarded. Thus, the combination of Rowney et al. and Oishi still does not teach the use of a unique transistory insignia which is provided to A by C conditioned on A providing to C a secret identification code so that B can validate the insignia

through C. Accordingly, Applicants submit that claim 1 overcomes this combination of references.

The remaining claims depend from claim 1 and as such are also considered to be allowable. In addition, each of these claims recite a number of other features of the invention, many of which are not seen in the references.

The world are seeing an increasing number of identity thefts and misuse of credit cards on the Internet. Everybody is looking for an easy, but secure solution. Most of todays payment systems use the Rowney solution or similar solution, but evidence has shown, that this kind of solution does not solve the problem of misuse of credit cards on the network.

In the following, without any doubt, it is seen that the invention differs fundamentally from Rowney's and Oishi and that the invention will secure the use of credit cards on the network and that the invention is not obvious as no one has yet come up with such a solution. As can be seen from Rowney column 1, lines 37–43 and lines 57–67, column 2, lines 7–19 and Objects of the invention column 2, lines 45–56, Rowney's invention deals and provides for a hybrid approach which encourage the deployment of a three-party secure channel such as SET by payment gateways in the absence of customer acceptance etc., etc. It is evident, that the objective and goal of the invention is not security but to overcome the lack of users accepting and using the SET-standard (which requires a software program being downloaded to the customer computer).

It is obvious, that the Rowney solution does not solve the problem as the world are seeing more and more fraud with credit cards on the Internet.

Contrary, the invention prevents fraud, is easy to implement and does not require any software program being downloaded to the customer computer.

Concerning Rowney column 10, lines 4 – 19, Rowney does not associate the payment transaction with a unique transitory insignia, but instead as a first step in establishing a communication between customer computer and merchant computer rely on an optional SSL certificate being sent to the merchant computer to verify the customer computer. The fact that the referenced certificate is optional has the effect in real life, that most customer computers does not have a certificate, causing that the verification insignia to verify the approval to B cannot be made. In the cited reference Rowney et al describes an overview of the Rowney invention and it is evident that there is no mentioning of associating a transaction with an insignia.

It is evident, that the SSL protocol distinguish between protocol elements/message and then application data. Application data can not be mixed with protocol elements/messages as can be seen from the extract below, which proves, that Rowney solution can not associate the payment transaction with the insignia.

Extract from The SSL Protocol, Version 3.0 by Alan O. Freier, Philip Karlton and Poul C. Kocher, paragraph 7.5 Handshake protocol overview:

> The client sends a **client hello** message to which the server must respond with a **server hello** message, or else a fatal error will occur and the connection will fail. The **client hello** and **server hello** are used to establish security enhancement capabilities between client and server. The **client hello** and **server hello** establish the following attributes: protocol version, session ID, cipher suite, and compression method. Additionally, two random values are generated and exchanged: ClientHello.random and ServerHello.random.
>
> Following the hello messages, the server will send its certificate, if it is to be authenticated. Additionally, a **server key exchange** message may be sent, if it is required (e.g. if their server has no certificate, or if its certificate is for signing only). If the server is authenticated, it may request a certificate from the client, if that is appropriate to the cipher suite selected.
>
> Now the server will send the **server hello done** message, indicating that the hello-message phase of the handshake is complete. The server will then wait for a client response.
>
> If the server has sent a **certificate request** message, the client must send either the **certificate message** or a **no certificate** alert. The **client key exchange** message is now sent, and the content of that message will depend on the public key algorithm selected between the **client hello** and the **server hello**. If the client has sent a certificate with signing ability, a digitally-signed **certificate verify** message is sent to explicitly verify the certificate.
>
> At this point, a **change cipher spec** message is sent by the client, and the client copies the *pending* Cipher Spec into the *current* Cipher Spec. The client then immediately sends the **finished** message under the new algorithms, keys, and secrets. In response, the server will send its own **change cipher spec** message, transfer the *pending* to the *current* Cipher Spec, and send its **Finished** message under the new Cipher Spec. At this point, the handshake is complete and the client and server may begin to exchange application layer data.

It can be seen that after the handshake is finished the two communicating parties can send application data, the contents of which is completely transparent for the protocol. So it is not possible to associate the transaction with the certificate (which is as mentioned earlier optional).

As a second step Rowney disclose that the customer computer sends a payment transaction to the merchant computer. But the payment transaction is not associated with a unique transitory insignia, which is evident when reading Rowney et al column 11, lines 45–58.

Concerning Rowney column 11, lines 30–37, Rowney et al does not disclose that the unique transitory insignia is provided to A by C, but describes the optional certificate in the context of the SSL-protocol. If customer computer does not have a certificate, customer computer may transmit a no-client-certificate alert, to indicate that the customer has not registered with any certification authority. Instead customer computer may transmit a a client key exchange message to be used by merchant computer system to decrypt further messages sent by customer computer system. It can therefore be derived, that in most cases A is not provided with a verification insignia from C and merchant computer can not authenticate the identity of customer computer system.

Furthermore, even if the customer computer sends a SSL certificate then it can not be used to verify the identity of the user of the customer computer, but can only verify that the customer computer contains a certificate. In fact anybody can sit down at the customer computer and send a payment transaction containing a false (stolen) credit card number, and the payment will be accepted. And that is what is happening to day.

Concerning Rowney et al column 15, lines 56–64, Rowney et al does not show B validating the insignia and upon positive validation accepts the transaction. When reading the cited reference it is evident, that the reference disclose that merchant computer (B) verifies payment computer C's digital certificate, by making a call to the certification authority

associated with the certificate. In other words, it is evident when reading the cited reference, that B does not validate any insignia from A and does not accept any transaction.

The Oishi invention describes a system providing a digital signature method capable of reliable ensuring anonymity under any circumstance for the safety of privacy protection by using a scheme of digital signatures and anonymous public key certificates.

In Oishi column 18, lines 22 – 32 it is stated:

> " In any of the above embodiments, safety of privacy protection can be further improved by performing the following operations.
> (1) The certificate publisher Q terminal device 20 transmits an anonymous public key certificate to an arbitrary user terminal device (e.g. user j terminal device 30), by using ueach time a different random number.
> (2) Upon reception of the anonymous public key certificate, the user j terminal device 30 does not generate a digital signature but uses one anonymous public key certificate for each different plain text".

It is quite unclear in the text, how this is actually performed. How does user terminal j obtain an anonymous public key certificate? How often and how is the processing done?

In the reference, Oishi does not disclose, that the insignia is invalidated immediately after validation. First of all nothing is said in the reference about validation of the anonymous public key certificate, secondly it is not invalidated but discarded, which is not at all the same. In our solution it is imperative, that the insignia is invalidated immediately after validation.

Furthermore, the Oishi invention deals with public key certificates and cryptosystems, which in no way has anything to do with payment systems on the Internet.

As pointed out above the invention is quite different from Rowney and Oishi, and also the transaction flow differs fundamentally.

In the invention a purchase is done in 2 steps, as follows.

A = customer computer

B = merchant computer

C = bank, creditcard company

Step 1. Obtaining a unique transitory insignia

A initiates a communication to C and by submitting a secret identification code to C confirming the identity of A (which is validated by C). On positive validation A is provided with a unique transitory insignia (which could be a one-time, virtual, short-lived credit card number).

Step 2. Making the purchase

A (customer) submits the received unique transitory insignia to B (merchant) as a means of payment. B validates the unique transitory insignia by contacting C. C verifies the unique transitory insignia and upon positive validation transmit a positive answer to B, and C invalidates the unique transitory insignia substantially immediately after the validation. B transmit a positive acknowledgement to A indicating that the purchase has been made.

The time between Step 1 and 2 is a matter of seconds.

From the above, Applicants submit that the arrangement of the devices of the present invention and that shown by Rowney et al. is completely different. Accordingly, Applicants submit that the claims as presently presented cannot be obvious over Rowney even when taken

in combination with any other references cited by the Examiner. Accordingly, Applicant submit that all of the claims should be allowed.

CONCLUSION

In view of the above remarks, it is believed that the claims clearly distinguish over the patents relied on by the Examiner, either alone or in combination. In view of this, reconsideration of the rejections and allowance of all of the claims is respectfully requested.

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone Robert F.Gnuse, Registration No. 27,295, at (703) 205-8076, in the Washington, D.C. area.

Prompt and favorable consideration of this Amendment is respectfully requested.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: September 19, 2005

Respectfully submitted,

By _____
Joe McKinney Muncy
Registration No.: 32,334
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Rd
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant